SECURITIES AND EXCHANGE COMMISSION
17 CFR Parts 229, 232, 239, 240, and 249
[Release Nos. 33-11038; 34-94382; IC-34529; File No. S7-09-22]
RIN 3235-AM89
Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure
AGENCY: Securities and Exchange Commission

Full text available here.

Request for Comment

1. Would investors benefit from current reporting about material cybersecurity incidents on Form 8-K? Does the proposed Form 8-K disclosure requirement appropriately balance the informational needs of investors and the reporting burdens on registrants?

   As a general statement, investors would certainly benefit from greater insight into cybersecurity incidents via Form 8-K. The time allowed before filing a Form 8-K may be problematic when dealing with complex cyber incidents that take more than four days to investigate. Public disclosure of an investigation may alter an adversary's tactics, if they are still executing their attack. If law enforcement is involved, investigations will almost certainly take more than four days. In the short run, it is my opinion that the need for discretion by investigators and law enforcement officials is of greater importance than an investor's need for early incident information. Once disclosure of an investigation no longer puts that effort at risk, disclosure via Form 8-K will provide the relevant information to investors.

   A gap that I see in the current language is the use of the word "material"? If left to individual companies to decide, materiality will vary greatly leaving investors in a position where they have more information, but it will be inconsistent across their portfolio. Some guardrails around the definition of materiality would be helpful in determining what cyber incidents must be reported via Form 8-K.

2. Would proposed Item 1.05 require an appropriate level of disclosure about a material cybersecurity incident? Would the proposed disclosures allow investors to understand the nature of the incident and its potential impact on the registrant, and make an informed investment decision? Should we modify or eliminate any of the specified disclosure items in proposed Item 1.05? Is there any additional information about a material cybersecurity incident that Item 1.05 should require?

   The information included in the draft Form 8-K would provide the average investor sufficient information to assess any impact to their investment strategy. One possible addition would be the estimated duration of the event, especially in the event of an aggregated cyber incident. The current information to be requested identifies when an incident was discovered; however, it does not specify disclosing if that incident has been affecting systems or data for a prolonged period.

3. Could any of the proposed Item 1.05 disclosures or the proposed timing of the disclosures have the unintentional effect of putting registrants at additional risk of future cybersecurity incidents? If so, how could we modify the proposal to avoid this effect? For example, should registrants instead provide some of the disclosures in proposed Item 1.05 in the registrant's next periodic report? If so, which disclosures?

   Four days is a very short period to investigate and determine the full effect of a complex cyber incident. Premature notification may cause an attacker to change tactics or clean up their tracks before investigators can prevent such actions. Notification of a cyber incident within four days of detection may also invite other attackers to take advantage of the situation. While a company is busy investigating and defending against one attack, a second attacker may find it easier to infiltrate the company through the same or different means than the first. Disclosure of a cyber incident prior to having a reasonable opportunity to closing the point of intrusion will increase the risk of a secondary incident. Postponing disclosure of remediation status or specific operational impacts until a later time would reduce that risk.

4. We are proposing to require registrants to file an Item 1.05 Form 8-K within four business days after the registrant determines that it has experienced a material cybersecurity incident. Would the proposed four-business day filing deadline provide sufficient time for registrants to prepare the disclosures that would be required under proposed Item 1.05? Should we modify the timeframe in which a registrant must file a Form 8-K under proposed Item 1.05? If so, what timeframe would be more appropriate for making these disclosures?

   Complex cyber incidents may not have completed their investigation withing four days of detection which would make the completion of Form 8-K impossible. Simple incidents that are wrapped up in four days or less wouldn't likely reach the threshold of being "material". A reporting window of thirty to sixty days would provide more opportunity for the company to complete an investigation and take necessary precautions to prevent a second attack utilizing the same point of entry. Form 8-K could still be utilized for that disclosure.

5. Should there be a different triggering event for the Item 1.05 disclosure, such as the registrant's discovery that it has experienced a cybersecurity incident, even if the registrant has not yet been able to determine the materiality of the incident? If so, which information should be disclosed in Form 8-K based on a revised triggering event? Should we instead require disclosure only if the expected costs arising from a cybersecurity incident exceed a certain quantifiable threshold, e.g., a percentage of the company's assets, equity, revenues or net income or alternatively a precise number? If so, what would be an appropriate threshold?

   Disclosure of security events that have not been deemed an incident with material impact would be a bad idea. The volume of notifications would quickly drown out a disclosure worth elevation and reporting. As noted before, there should be some definition of materiality to guide companies on what warrants disclosure. Measures based on a percentage of assets, revenues, income, or other scalable data points would be recommended to leverage a single scale across companies of various sizes. There may also be non-numerical measures based on

the market vertical that the company is apart of.

6. To what extent, if any, would the proposed Form 8-K incident reporting obligation create conflicts for a registrant with respect to other obligations of the registrant under federal or state law? How would any such conflicting obligations arise, and what mechanisms could the Commission use to ensure that registrants can comply with other laws and regulations while providing these timely disclosures to investors? What costs would registrants face in determining the extent of a potential conflict?

   No comment.

7. Should any rule provide that the Commission shall allow registrants to delay reporting of a cybersecurity incident where the Attorney General requests such a delay from the Commission based on the Attorney General's written determination that the delay is in the interest of national security?

   Any request from the Attorney General, a court, or federal law enforcement should pause the disclosure requirements under this rule change.

8. We are proposing to include an instruction that "a registrant shall make a materiality determination regarding a cybersecurity incident as soon as reasonably practicable after discovery of the incident." Is this instruction sufficient to mitigate the risk of a registrant delaying a materiality determination? Should we consider further guidance regarding the timing of a materiality determination? Should we, for example, suggest examples of timeframes that would (or would not), in most circumstances, be considered prompt?

   Depending upon the definition of materiality and the data points required to calculate it, some companies may not be able to adequately calculate such a measure regardless of the timeline.

9. Should certain registrants that would be within the scope of the proposed requirements, but that are subject to other cybersecurity-related regulations, or that would be included in the scope of the Commission's recently-proposed cybersecurity rules for advisers and funds, if adopted, be excluded from the proposed requirements? For example, should the proposed Form 8-K reporting requirements or the other disclosure requirements described in this release, as applicable, exclude business development companies ("BDCs"), or the publicly traded parent of an adviser?

   No comment.

10. As described further below, we are proposing to define cybersecurity incident to include an unauthorized occurrence on or through a registrant's "information systems," which is proposed to include "information resources owned or used by the registrant." Would registrants be reasonably able to obtain information to make a materiality determination about cybersecurity incidents affecting information resources that are used but not owned by them? Would a safe

harbor for information about cybersecurity incidents affecting information resources that are used but not owned by a registrant be appropriate? If so, why, and what would be the appropriate scope of a safe harbor? What alternative disclosure requirements would provide investors with information about cybersecurity incidents and risks that affect registrants via information systems owned by third parties?

Depending upon the definition of materiality and the data points required to calculate it, some companies may not be able to adequately calculate such a measure. If properly defined, it will be more difficult for a company to claim an inability to estimate the materiality of a cyber incident. A refined, financial quantification of a cyber incident is a mature capability that many companies have decided not to invest in due to competing priorities.

11. We are proposing that registrants be required to file rather than permitted to furnish an Item 1.05 Form 8-K. Should we instead permit registrants to furnish an Item 1.05 Form 8-K, such that the Form 8-K would not be subject to liability under Section 18 of the Exchange Act unless the registrant specifically states that the information is to be considered "filed" or incorporates it by reference into a filing under the Securities Act or Exchange Act?

    No comment.

12. We note above a non-exclusive list of examples that would merit disclosure under Item 1.05 of Form 8-K covers some, but not all, types of material cybersecurity incidents. Are there additional examples we should address? Should we include a non-exclusive list of examples in Item 1.05 of Form 8-K?

    As for the types of incidents, the list is well crafted. Materiality must still be incorporated before determining the need to disclose. For example, a single laptop being infected with ransomware would not be worth disclosing; however, 50% of a company being infected and a ransom demanded would certainly warrant disclosure.

13. Should we include Item 1.05 in the Exchange Act Rules 13a-11 and 15d-11 safe harbors from public and private claims under Exchange Act Section 10(b) and Rule 10b-5 for failure to timely file a Form 8-K, as proposed?

    No comment.

14. 14. Should we include Item 1.05, as proposed, in the list of Form 8-K items where failure to timely file a Form 8-K will not result in the loss of a registrant's eligibility to file a registration statement on Form S-3 and Form SF-3?

    No comment.

15. Should we require registrants to disclose any material changes or updates to information that would be disclosed pursuant to proposed Item 1.05 of Form 8-K in the registrant's quarterly or

annual report, as proposed? Are there instances, other than to correct inaccurate or materially misleading prior disclosures, when a registrant should be required to update its report on Form 8-K or file another Form 8-K instead of providing disclosure of material changes, additions, or updates in a subsequent Form 10-Q or Form 10-K?

Updates on a cyber incident should be included in an updated Form 8-K. A summary of filed Form 8-Ks should be included in the quarterly and annual reports.

16. Should we require a registrant to provide disclosure on Form 10-Q or Form 10-K when a series of previously undisclosed and individually immaterial cybersecurity incidents becomes material in the aggregate, as proposed? Alternatively, should we require a registrant to provide disclosure in Form 8-K, rather than in a periodic report, as proposed, when a series of previously undisclosed and individually immaterial cybersecurity incidents becomes material in the aggregate?

    A series of immaterial cyber incidents that reveal an systemic issue with material impact should be disclosed via Form 8-K as though it were a singular cyber incident with material impact. Many cyber incidents begin with smaller events that culminate with a large incident.

17. Should we adopt Item 106(b) and (c) as proposed? Are there other aspects of a registrant's cybersecurity policies and procedures or governance that should be required to be disclosed under Item 106, to the extent that a registrant has any policies and procedures or governance? Conversely, should we exclude any of the proposed Item 106 disclosure requirements?

    The existence of cybersecurity policies and procedures is warranted and provide a baseline level of information to an investor that the company is taking the necessary threats into due consideration. I would not, however, advise that companies be required to disclose the contents of those policies or procedures. If an attacker understands the methods that a company uses to prevent, detect, and respond to cyber incidents, they will be able to adjust their tactics to evade detection.

18. Are the proposed definitions of the terms "cybersecurity incident," "cybersecurity threat," and "information systems," in Item 106(a) appropriate or should they be revised? Are there other terms used in the proposed amendments that we should define?

    The definitions suit the current scope of the proposed rule changes.

19. The proposed rule does not define "cybersecurity." We could define the term to mean, for example: "any action, step, or measure to detect, prevent, deter, mitigate, or address any cybersecurity threat or any potential cybersecurity threat." Would defining "cybersecurity" in proposed Item 106(a) be helpful? Why or why not? If defining this term would be helpful, is the definition provided above appropriate, or is there another definition that would better define "cybersecurity"?

I do not believe that defining “cybersecurity” is particularly necessary. There is a generally accepted definition of cybersecurity that exceeds the boundaries of what is considered in this proposed rule change.

20. Should we require the registrant to specify whether any cybersecurity assessor, consultant, auditor, or other service that it relies on is through an internal function or through an external third-party service provider? Would such a disclosure be useful for investors?

    Such details would not be useful to an investor. Investors should be concerned with whether or not the company is employing tactics to reduce their cybersecurity risk posture, not the type of badge an individual wears when completing the work.

21. As proposed, a registrant that has not established any cybersecurity policies or procedures would not have to explicitly state that this is the case. If applicable, should a registrant have to explicitly state that it has not established any cybersecurity policies and procedures?

    Yes. This disclosure would be particularly pertinent to an investor because it identifies a very low level of maturity that could be a major concern for many investors.

22. Are there concerns that certain disclosures required under Item 106 would have the potential effect of undermining a registrant’s cybersecurity defense efforts or have other potentially adverse effects by highlighting a registrant’s lack of policies and procedures related to cybersecurity? If so, how should we address these concerns while balancing investor need for a sufficient description of a registrant’s policies and procedures for purposes of their investment decisions?

    As stated above, the existence of cybersecurity policies and procedures is warranted and provide a baseline level of information to an investor that the company is taking the necessary threats into due consideration. I would not, however, advise that companies be required to disclose the contents of those policies or procedures. If an attacker understands the methods that a company uses to prevent, detect, and respond to cyber incidents, they will be able to adjust their tactics to evade detection.

23. Should we exempt certain categories of registrants from proposed Item 106, such as smaller reporting companies, emerging growth companies, or FPIs? If so, which ones and why? How would any exemption impact investor assessments and comparisons of the cybersecurity risks of registrants? Alternatively, should we provide for scaled disclosure requirements by any of these categories of registrants, and if so, how?

    I recommend the same reporting requirements for all publicly traded companies regardless of size and market vertical.

24. Should we provide for delayed compliance or other transition provisions for proposed Item 106 for certain categories of registrants, such as smaller reporting companies, emerging growth

companies, FPIs, or asset-backed securities issuers? Proposed Item 106(b), which would require companies to provide disclosures regarding existing policies and procedures for the identification and management of cybersecurity incidents, would be required in annual reports. Should the proposed Item 106(b) disclosures also be required in registration statements under the Securities Act and the Exchange Act?

I recommend the same reporting requirements for all publicly traded companies as of the day that they become publicly traded.

25. To what extent would disclosure under proposed Item 106 overlap with disclosure required under Item 407(h) of Regulation S-K ("Board leadership structure and role in oversight") with respect to board oversight of cybersecurity risks? To the extent there is significant overlap, should we expressly provide for the use of hyperlinks or cross-references in Item 106? Are there other approaches that would effectively decrease duplicative disclosure without being cumbersome for investors?

    No comment.

26. Would proposed Item 407(j) disclosure provide information that investors would find useful? Should it be modified in any way?

    The proposed information would be useful to an informed investor as it identifies the experience of directors in the field of cybersecurity, be it as a practitioner or executive.

27. Should we require disclosure of the names of persons with cybersecurity expertise on the board of directors, as currently proposed in Item 407(j)(1)? Would a requirement to name such persons have the unintended effect of deterring persons with this expertise from serving on a board of directors?

    Since directors are disclosed by name in other filings, a description of one's background would be easy to match based on other publicly available information. I do not believe that disclosing a director's name, along with the background in these forms, would be a deterrent to serving on a board.

28. When a registrant does not have a person with cybersecurity expertise on its board of directors, should the registrant be required to state expressly that this is the case under proposed Item 407(j)(1)? As proposed, we would not require a registrant to make such an explicit statement.

    If a board does not have a director with cybersecurity experience, I would recommend requiring a response as to how the company fills that experience void. The company may leverage internal executives or non-voting advocates when cybersecurity subjects require attention.

29. Proposed Item 407(j) would require registrants to describe fully the nature of a board member's expertise in cybersecurity without mandating specific disclosures. Is there particular information

that we should instead require a registrant to disclose with respect to a board member's expertise in cybersecurity?

The recommended information appears to be a good starting point that may warrant amendments over time.

30. As proposed, Item 407(j)(1) includes a non-exclusive list of criteria that a company should consider in determining whether a director has expertise in cybersecurity. Are these factors for registrants to consider useful in determining cybersecurity expertise? Should the list be revised, eliminated, or supplemented?

    No changes recommended at this time.

31. Would the Item 407(j) disclosure requirements have the unintended effect of undermining a registrant's cybersecurity defense efforts or otherwise impose undue burdens on registrants? If so, how?

    No.

32. Should 407(j) disclosure of board expertise be required in an annual report and proxy or information statement, as proposed?

    The information should be included in the annual report alongside other pertinent company information.

33. To what extent would disclosure under proposed Item 407(j) overlap with disclosure required under Item 401(e) of Regulation S-K with respect to the business experience of directors? Are there alternative approaches that would avoid duplicative disclosure without being cumbersome for investors?

    No comment.

34. As proposed, Item 407(j) does not include a definition of the term "expertise" in the context of cybersecurity? Should Item 407(j) define the term "expertise"? If so, how should we define the term?

    Since there is not a minimum requirement that is demanded of a director, expertise simply refers to the level of knowledge that the individual possesses on the subject. No further definition is really required at this time.

35. Should certain categories of registrants, such as smaller reporting companies, emerging growth companies, or FPIs, be excluded from the proposed Item 407(j) disclosure requirement? How would any exclusion affect the ability of investors to assess the cybersecurity risk of a registrant or compare such risk among registrants?

I recommend the same reporting requirements for all publicly traded companies regardless of size and market vertical.

36. Should we adopt the proposed Item 407(j)(2) safe harbor to clarify that a director identified as having expertise in cybersecurity would not have any increased level of liability under the federal securities laws as a result of such identification? Are there alternatives we should consider?

    No comment.

37. As proposed, disclosure under Item 407(j) would be required in a proxy or information statement. Should we require the disclosure under Item 407(j) to appear in a registrant's proxy or information statement regardless of whether the registrant is relying on General Instruction G(3)? Is this information relevant to a security holder's decision to vote for a particular director?

    No comment.

38. Should we amend Form 20-F, as proposed to require disclosure regarding cybersecurity risk management and strategy, governance, and incidents? Additionally, should we amend Form 6-K, as proposed, to add "cybersecurity incidents" as a reporting topic? Are there unique considerations with respect to FPIs in these contexts?

    No comment.

39. We are not proposing any changes to Form 40-F. Should we instead require an MJDS issuer filing an annual report on Form 40-F to comply with the Commission's specific proposed cybersecurity-related disclosure requirements in the same manner as Form 10-K or Form 20- F filers?

    No comment.

40. Should we require registrants to tag the disclosures required by proposed Item 1.05 of Form 8-K and Items 106 and 407(j) of Regulation S-K in Inline XBRL, as proposed? Are there any changes we should make to ensure accurate and consistent tagging? If so, what changes should we make? Should we require registrants to use a different structured data language to tag these disclosures? If so, what structured data language should we require? Are there any registrants, such as smaller reporting companies, emerging growth companies, or FPIs that we should exempt from the tagging requirement?

    Tagging will make analysis by informed investors faster and more consistent. No recommended changes at this time.

41. What are the economic effects of the proposed cybersecurity incident and cybersecurity risk management, strategy, and governance disclosures? Would those disclosures provide informational benefits to investors? Would registrants benefit from a potential decrease in cost of capital because of the enhanced disclosure? Are there any other benefits, costs, and indirect effects of the proposed disclosure that we should also consider?

    Any additional information that is provided to investors will prove useful; however, incomplete information may result in investors drawing inaccurate conclusions. Increased disclosure requirements will result in increased costs for the registrants regardless of the economic theory reviewed. Additional costs will be incurred to execute disclosure processes and resolve questions and disputes that arise from said disclosures. Companies with strong risk management and cybersecurity capabilities may not incur additional capital costs, the notion that they may see a reduction in capital costs due to increased disclosures is unrealistic.

42. Would the proposed cybersecurity incident disclosure provide enough information for investors to assess the impact of a cybersecurity incident in making an investment decision? Because the proposed incident disclosure would not require quantification of an incident's impact, would the lack of quantification create any uncertainty for investors which may cause them to under or overreact to the disclosure? Would investors benefit more if registrants were to provide the disclosure after the incident's impact is quantified or can be reasonably estimated? If so, what metrics should be disclose to help investors understand the impact?

    Quantification of the impact of a cyber incident would provide a significantly improved view of the impact to the company if the unit of measure is consistent across companies. Investors will be looking at these disclosures, along with other data inputs, to make comparisons between possible investments. A common unit of measure is the best means of supporting that decision process. In the absence of quantification, investors will need to evaluate the subjective information for themselves based on their own knowledge of cybersecurity.

43. Would both types of the proposed disclosure, cybersecurity incident disclosure and cybersecurity risk management, strategy, and governance disclosure, increase the vulnerability of registrants to cybersecurity incidents? Would this effect be mitigated by any of the other effects of the proposal, including indirect effects such as registrants' potential strengthening of cybersecurity risk management measures? What would be the impact of the proposed disclosure on the likelihood of future incidents for registrants? Would that impact be the same for both types of disclosure?

    There is an immediate and greater potential impact on a registrant's disclosure of a cyber incident within 4 days of discovery. Few organizations will be able to fully remediate or mitigate a significant vulnerability prior to disclosure, which will create an opportunity for other attacks. There are long term benefits from improvements in a company's risk management and cyber capabilities, which should reduce the potential impact and likelihood of a cyber incident; however, there are short term increases to both risk and likelihood.

There is a potential impact that disclosing what policies and procedures are in place will reveal a weakness in the company's security posture. This could disclose a vulnerability that an attacker could take advantage of thus creating a new cyber incident as a result of the disclosure. It is important to note that the company, in this situation, is already at risk of a cyber incident; however, the disclosure would expose that vulnerability to the general public.

44. Would the proposed incident disclosure increase registrants' compliance costs to fulfill the proposed disclosure requirements related to incident reporting? What would be the magnitude of those costs? Would the proposed cybersecurity risk management, strategy, and governance disclosure lead to indirect costs such as hiring a board member or staff to their management team with cybersecurity expertise, or costs to devise, implement or improve the processes and procedures related to cybersecurity?

    Additional costs will be incurred to execute disclosure processes and resolve questions and disputes that arise from said disclosures. The magnitude of those costs is not going to be uniform across companies. Various industries have existing disclosure requirements in place, some have voluntary disclosure processes with information sharing exchanges, while others have little to no external disclosure processes. Additional costs could include hiring additional personnel on the board of directors or support staff, if such personnel do not already exist within the company. Companies with less mature cybersecurity programs will likely see pressure for additional investments in cyber capabilities.

45. Would both types of the proposed disclosure lead to indirect economic effects for external stakeholders? Would the magnitude of the indirect effects be greater or less than we have discussed? Are there any other indirect effects that we should consider?

    No comment.

46. Are there any specific data points that would be valuable for assessing the economic effects of the proposed cybersecurity incident and risk management, strategy, and governance that we should consider in the baseline analysis or the analysis of the economic effects? If so, please provide that data.

    No comment.

47. Would any of the economic effects discussed above be more or less significant than in our assessment? Are any of the costs or benefits identified incorrectly for any of the proposed amendments? Are there any other economic effects associated with these proposed rules that we should consider? Are you aware of any data or methodology that can help quantify the benefits or costs of the proposed amendments?

    No comment.

48. Would any of the proposed amendments positively affect efficiency, competition and capital formation as we have discussed? Are there any other effects on efficiency, competition, and capital formation that we should consider?

    No comment.

49. Would any of the proposed amendments have disproportionate costs for smaller reporting companies? Do smaller reporting companies face a different set of cybersecurity risks than other companies?

    Each company has a unique risk profile based on the internal threats, external threats, existing capabilities, market, geolocation, etc. Smaller companies definitely possess a different set of cybersecurity risks than larger counterparts in the same industry. Smaller companies typically have smaller cybersecurity programs which will likely find external disclosures more difficult to complete on schedule. The same personnel that are responsible for investigating the cyber incident will likely be responsible for conducting the external disclosure.

50. Are there any other alternative approaches to improve disclosure of material cybersecurity incidents, cybersecurity risk management, strategy, or governance that we should consider? If so, what are they and what would be the associated costs or benefits of these alternative approaches?

    The primary concern that I have with the proposal, as laid out, is the timing of the disclosure. Investors have a right to be informed of the cybersecurity posture a company has if they are considering making an investment in that company. That need for information does not outweigh the need for the company and law enforcement resources to conduct a proper investigation. Furthermore, a company should have the right to remediate or mitigate exploited vulnerabilities prior to public disclosure of a cyber incident. I would propose altering the timeline for disclosure and providing for an elongated timeline when deemed necessary by law enforcement.

51. Are there any other costs and benefits associated with alternative approaches that are not identified or are misidentified in the above analysis? Should we consider any of the alternative approaches outlined above instead of the proposed rules? Which approach and why?

    No recommendations at this time.